Case study on ping sweeps and port scans

Law, Security

\n[toc title="Table of Contents"]\n

\n \t

\n[/toc]\n \n

Ping Sweeps and Port Scans

Introduction

Every information infrastructure of any organization is target for hackers. Hackers will always come up with new ways of trying to gain access to the network whether internally or externally. Some of the techniques that have been employed by intruders include ping sweeps and port scans (Baskin, & Kanclirz, 2008). They use these means to access network information, which would be instrumental for them in the process of hacking.

Ping sweeps

Ping sweeps is a major way through which hackers will gain access to network resources. Every IT professional should be worried about the possibility of the same happening to his or her resources. Ping sweep is used to determine the range of network IPs, which is associated to working nodes or hosts. This networking terminology employs a scanning mechanism on the network in order to determine the hosts on the same network. A request is

sent to the entire network during the process of pinging. This request is based on the Internet Control Message Protocol (ICMP) echo (Baskin, & Kanclirz, 2008). A reply is always given by live machines on the network. If any machine is not online, then no reply will be received. After identifying the machines that are online, a hacker can focus on hacking into the selected system then.

Though ping sweeps is largely associated with hackers, it is important to note that the same is an administrative task, which can be employed by a network or systems administrator while diagnosing the network (White, 2003).

Port scans

Just like ping sweeps, port scan is a technology mostly used by hackers. It is used to identify a service of interest which hackers find it worth attacking. Systems logs can be instrumental in identifying port scan done. Scans are done by sending messages to different ports. These ports are sometimes known or unknown to the host. In addition, some ports are used while others are not used. In essence, when a reply is received from the probed port, an attacker can then continue probing it to identify weaknesses associated with it (McNab, 2004). When a weakness is identified, a potential hacker would then capitalize on the found advantage to hack in to the system.

There is need for management to develop effective mechanisms in order to overcome the risks associated with port scans and ping sweeps. A number of detection systems that can be used to curb these risks. Intrusion detection system can be used to detect Ping sweeps. Another way of trying to solve the problem is to turn off the ping sweep and only turn t on when need be;

when systems administrator wants to perform a diagnostic run (White, 2003).

The company need not to worry about the risks associated with these threats since the same can be identified and mitigated at early stages. Implementation of firewalls can also serve to curb external port scans. The methods discussed previously can be used to prevent these risks.

Conclusion

Ping sweeps and port scans are commonly used by hackers in the IT industry. Though the same is a threat, there are adequate potential ways that can be use to control. Systems administrators need to put in place preventive, detection as well as recovery mechanism as a remedy to the threat. Other ways of testing network connectivity should also be used by administrators, and avoid the use of ping sweeps which can also be used by hackers.

Reference

Baskin B., & Kanclirz, J. (2008). Netcat Power Tools. New York, NY: Syngress

McNab, C. (2004). Network Security Assessment. Sebastopol, CA: O'Reilly .

White, G. (2003). Security + in information systems. Emeryville, CA: McGraw-

Hill/Osborne.